PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/08, G07D 7/00 — A1

(11) International Publication Number: **WO 00/23954**

(43) International Publication Date: 27 April 2000 (27.04.00)

(21) International Application Number: PCT/GB99/03377

(22) International Filing Date: 11 October 1999 (11.10.99)

(30) Priority Data:
9822626.9 17 October 1998 (17.10.98) GB

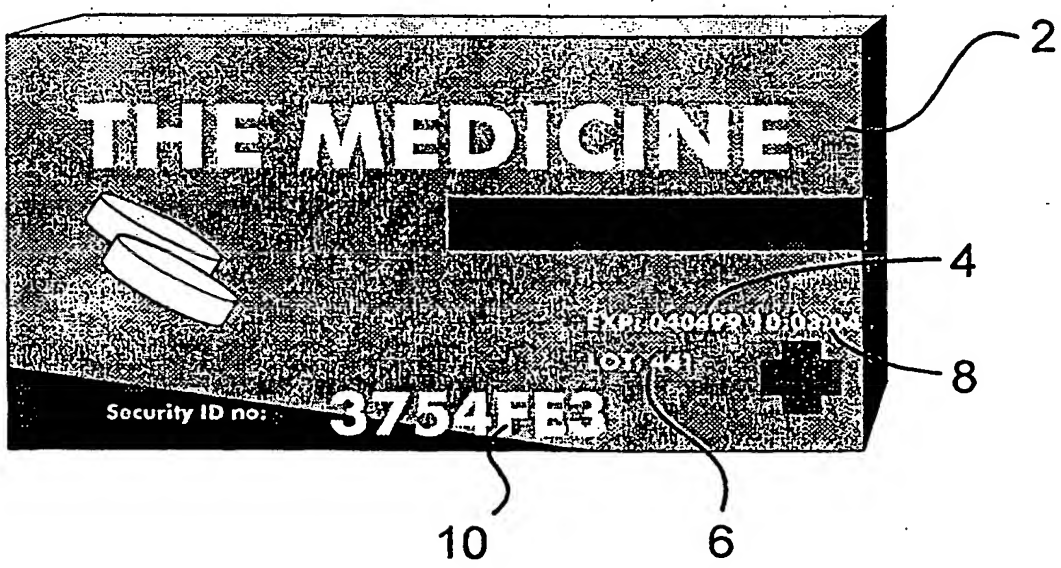
(71)(72) Applicants and Inventors: ELLIOTT, Nicholas, Paul [GB/GB]; Shoestring, Woodford Mill, Ringstead, Kettering Northants NN14 4DU (GB). ELLIOTT, David, William [GB/GB]; Rosedene, 2 Coleman Street, Raunds, Northants NN9 6NJ (GB).

(74) Agent: RAYNOR, Simon, Mark; Urquhart-Dykes & Lord, Midsummer House, 411C Midsummer Boulevard, Central Milton Keynes, Bucks MK9 3BN (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: VERIFICATION METHOD



(57) Abstract

A method of verifying the authenticity of goods is provided, wherein a set of public data (4, 6, 8) and security code (10) are applied to the goods (2), said security code having been derived from said public data by means of a predetermined encryption algorithm. Upon receiving a request for verification, the public data (4, 6, 8) applied to the goods (2) is entered into the predetermined encryption algorithm to generate a verification code. The verification code is then compared with the security code (10) applied to the goods to assess the authenticity of goods.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

VERIFICATION METHOD

The present invention relates to a verification method and in particular, but not exclusively, to a method of verifying products to ensure that they are genuine and not counterfeit. The invention also relates to a method of marking goods for verification purposes and to goods marked for verification purposes.

The problem of counterfeiting is enormous and affects a wide range of goods including, for example, pharmaceuticals and spare parts for aircraft. Counterfeiting is not only bad for the producer of genuine goods, resulting in lost sales and possible damage to reputation and goodwill, but can also result in danger to the public if the counterfeit goods are not up to the quality of the genuine goods. For example, counterfeit pharmaceuticals may be ineffective or contain harmful substances and counterfeit aircraft parts may fail during use.

The sophistication of counterfeiting methods is such that it is often difficult or impossible for the consumer, wholesaler, retailer, importer or distributor to tell whether the goods are genuine or counterfeit, and usually there is no way of verifying the authenticity of the goods.

It is an object of the invention to provide a verification method and a method of marking goods for verification purposes that mitigates at least some of the aforesaid problems.

According to the present invention there is provided a method of verifying the authenticity of goods, wherein:

- a set of public data and a security code are applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm;
- and, upon receiving a request for verification, the public data applied to the goods is entered into said predetermined encryption algorithm to generate a verification code, and said verification code is compared with the security code applied to the goods to assess the authenticity of goods.

The set of public data and the security code may be applied to the goods themselves or to packaging for the goods and the invention as defined by claim 1 is intended to include both of these possibilities.

The method allows the authenticity of the goods to be verified very quickly and simply, for example by means of a telephone call to the verifier. Counterfeiting of the goods is made very difficult by the fact that each goods item carries a unique security code number. The security code can be applied to the goods by ordinary printing processes at minimal cost. The need for expensive security devices such as holograms is avoided.

Advantageously, said security code is derived from said public data applied to the goods and private data held by the verifier and, upon receiving a request for verification, the public data applied to the goods and private data held by the verifier are entered into said predetermined encryption algorithm to generate a verification code, and said verification code is compared with the security code applied to the goods to assess the authenticity of goods.

The verifier may be either the manufacturer or any other body authorised by the manufacturer and the term "verifier" as used in the claims is intended to include any such body.

The private data may be related to public data, for example to batch number, so enabling the verifier to assign different sets of private data to different batches of products. Then, when a request for verification is received, the verifier can select the appropriate set of private data for the particular goods for which verification has been requested.

The use of private data in addition to the public data applied to the goods increases the security of the encryption process, making it more difficult to counterfeit the goods.

Advantageously, said private data includes a plurality of private data sets and, upon receiving a request for verification, each private data set is entered into said predetermined encryption algorithm together with the public data applied to the goods to generate a list of verification codes, and said list of verification codes is compared with the security code applied to the goods to assess the authenticity of goods.

Each set of private data may be unique for each goods item, enabling the item number to be identified. This can help the verifier to track the activities of counterfeiters.

The public data may include a batch number and/or date information, for example the expiry date or the manufacturing date and time.

The private data may include an item number, allowing the verifier to identify the goods item in question, or it may be a random or pseudo-random number.

Advantageously, the public data and the private data is applied to the goods by means of a digital printing process and is incorporated into the design printed onto the goods. This makes it more difficult for the goods to be counterfeited using plate-based printing techniques.

Advantageously, the public data and the private data is incorporated into the design printed onto the goods as reversed out characters, blends or tints. This makes it more difficult for the goods to be counterfeited using over-printing or over-coding techniques.

According to a further aspect of the invention there is provided a method of marking goods to enable the authenticity of those goods to be verified, wherein a set of public data and a security code are applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm.

According to a further aspect of the invention there are provided goods marked for verification purposes, each of said goods including a set of public data and a security code applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm.

Embodiments of the invention will now be described by way of example with reference to the accompanying drawings, in which:

Fig. 1 is a perspective view of a medicine packet that has been marked for verification purposes,

Fig. 2 represents schematically a method of marking goods for verification purposes, and

Fig. 3 represents schematically a method of verifying the marked goods.

An example of a product, in this case a medicine packet 2, that has been marked for verification purposes is shown in Fig. 1. In the usual way, the packet has been marked by the manufacturer with information such as the expiry date 4, which in this case includes both the date and a time, and a lot or batch number. This information, which is printed on the packet in such a way that it can be read by the public, will be referred to hereinafter as the "public data" 8. This public data 8 may be either unique to each packet (for example, an item number may be included or the expiry date may include a time code based on the exact time of manufacture), or alternatively all packets manufactured in the same batch may carry identical public data.

In addition, the packet carries a security code 10. The security code 10 is unique to that packet and every packet therefore carries a different security code. The provision of a unique security code provides a first obstacle to counterfeiting, since printing different codes on each pack demands adaptable printing techniques and the provision of identical security codes on any two packets will immediately indicate that the goods are not genuine.

The usual method of marking packets with information that varies from pack to pack, or from batch to batch, is to stamp or print that variable information onto pre-printed packets in a separate printing process. This process is known as over-coding. This method can be copied relatively easily by counterfeiters.

In the packet shown in Fig. 1, counterfeiting is made more difficult by using digital printing techniques to print both the design of the packet (including the product trade mark, any descriptive matter and any graphical elements) and the variable information in a single step. Many well known digital printing techniques may be employed, including for example the INDIGO (TM), XEIKON (TM) and SCITEX (TM) processes. The advantage of using a digital printing process is that because printing takes place under digital electronic control, the printed image can be varied for each individual packet and can be incorporated into the overall design of the pack. This cannot readily be achieved

with traditional plate-based printing processes, since a separate set of printing plates must be prepared for each different image.

Preferably, the variable information including the public data and the security code is incorporated into the design in such a way that would affect as many plates of a conventional printing process as possible. For example, in the packet shown in Fig. 1 the security code number 10 has been positioned to overlap areas of two different background colours. Further, the variable information has been incorporated into the design as "reversed out" characters, i.e. characters produced by leaving the shapes of those characters unprinted against a background of solid colour so that the base material shows through. This helps to prevent that information being added in a subsequent over-coding process. The effect of this process is illustrated in Fig. 1, the variable information 8,10 being shown as white characters on a coloured background. Alternatively, the characters may be printed as blends or tints, which are also difficult to reproduce using conventional printing processes.

The security code 10 applied to each packet is derived directly from unique information associated with each pack by means of a secret encryption algorithm. The security code 10 may be derived either from a combination of the public data 8 printed on the packet 2 and private data held by the manufacturer or an authorised verifying organisation, or alternatively it may be derived solely from the public data, if that data is unique. The processes for deriving and verifying the security codes applied to the packets are described below with reference to Figs. 2 and 3.

Fig. 2 illustrates schematically a process for deriving the security codes and applying them to the packets using a combination of the public data 8 printed on the packet 2 and private data 12 held by the manufacturer or an authorised verifying organisation. The public data 8 consists for example of the batch number 6 and the expiry date 4. This data need not be unique. The private data 12 is not printed on the packet and is held either by the manufacturer or an authorised verifying organisation. The private data 12 is unique and may represent, for example, the item number of each packet in a given batch, or may be a random or pseudo-random number.

The security code 10 for each packet is derived automatically during the printing process by subjecting the private data 12 and the public data 8 to an encryption process 14, such as a one-way hash function or a merge digest, as described in Applied Cryptography, second edition by Bruce Schneier, page 30, section 2.4 "one-way hash functions" (John Wiley & Sons, Inc., 1996) ISBN 0471117091. This generates a unique security code 10, which is printed onto the packet 2 together with the public data 8 by means of a digital printer 18.

No record is kept of the security codes 10. However, a data record 20 is kept of the public data 8 and the associated private data 12 used in the encryption process. This data record 20 is supplied to the verifying authority, for example on a floppy disk or by electronic data transfer.

The verification process is illustrated schematically in Fig. 3. The verifying authority, which may the manufacturer or an outside body authorised by the manufacturer, uses an identical encryption algorithm 14 to that used during printing and is supplied with the data record 20 of public data 8 and private data 12. When the verifying authority receives a request for verification, for example from a member of the public who has purchased the goods, the requester is asked to provide the public data 8 printed on the packet 2. This public data 8 is entered into the encryption algorithm 14 together with the private data 12 associated with that public data 8, as retrieved from the data record 20. This generates a list 24 of possible verification codes and the private data associated with each of those codes.

The requester is then asked to provide the security code 10 printed on the packet 2 and this code 10 is compared 26 with the list 24 of verification codes generated by the encryption algorithm 14. If that security code 10 matches a verification code on the list 24, the authenticity of the goods is verified 28: if a match is not found, the authenticity of the goods is denied.

The verifier may keep a log 30 of all requests for verification, which stores the public and private data for each item that has been verified. During the verification step, the log 30 may be checked to see whether a request for verification has been received previously in

respect of that item. If so, verification may be denied since this suggests that the item has been copied.

The log 30 may also contain other information 32, for example the date and time of the request and the identity and geographical location of the requester. If two requests for verification are made for the same item, it may be possible to discount any likelihood of the item being counterfeit, for example if the requests are made first by a retail pharmacist and subsequently by a customer of that pharmacist.

A request for verification may be made by post, fax or telephone or electronically, for example by accessing a Web Site.

As mentioned above, the security code 10 applied to each packet 2 may be derived solely from the public data 8 printed on the packet 2, if that data is unique. For example, the public data may include a unique item number, the exact production time or a random number in addition to the normal batch number 6 and expiry date information 4. The security code 10 is derived directly from this combination of unique and non-unique data and by means of the encryption algorithm 14.

During the verification process, the requester provides the public data 8 printed on the pack and this is entered into the encryption algorithm by the verifier, thereby generating a verification code. The requester then provides the security code 10 printed on the pack and, if this matches the verification code generated by the verifier, the authenticity of the goods is confirmed. If the security code provided by the requester does not match the verification code, authenticity is denied. As in the process described above, a log may be kept of requests for verification and details of the requester.

The verification process is not limited to pharmaceuticals or to goods sold in printed packs and is equally applicable to goods such as aircraft parts, on which the public data 8 and the security code 10 may be marked directly, for example by stamping. In the case of goods sold in printed packs, the use of digital printing methods is not essential, although it is preferred as this provides certain additional advantages as discussed above.

It is not essential that the public data from which the security code is derived includes either the product batch number or date information. The public data may be entirely random or pseudo-random, or may be derived from the batch and item numbers, for example by means of a two-way algorithm.

The public data and the security code can also be amalgamated into a single number according to a predetermined algorithm. In order to verify the authenticity of the goods, the requester only has to provide that number. The verifier can automatically separate the public data from the security code and then use the public data extracted from that number to generate a verification code, which can then be compared with the security code extracted from the number provided on the goods. Verification can thus be achieved in a single step.

Claims

1. A method of verifying the authenticity of goods, wherein:

- a set of public data and a security code are applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm;

- and, upon receiving a request for verification, the public data applied to the goods is entered into said predetermined encryption algorithm to generate a verification code, and said verification code is compared with the security code applied to the goods to assess the authenticity of goods.

2. A method according to claim 1, wherein said security code is derived from said public data applied to the goods and private data held by the verifier and, upon receiving a request for verification, the public data applied to the goods and private data held by the verifier are entered into said predetermined encryption algorithm to generate a verification code, and said verification code is compared with the security code applied to the goods to assess the authenticity of goods.

3. A method according to claim 2, wherein said private data includes a plurality of private data sets and, upon receiving a request for verification, each private data set is entered into said predetermined encryption algorithm together with the public data applied to the goods to generate a list of verification codes, and said list of verification codes is compared with the security code applied to the goods to assess the authenticity of goods.

4. A method according to any one of the preceding claims, wherein the verifier maintains a log of requests for verification and, upon receiving a request for verification, compares the public data applied to the goods with the data held in the log to assess the authenticity of goods.

5. A method according to any one of the preceding claims, wherein the public data includes a batch number.

6. A method according to any one of the preceding claims, wherein the public data includes date information.

7. A method according to any one of the preceding claims, wherein the private data includes an item number.

8. A method according to any one of the preceding claims, wherein said public data and said private data is applied to the goods by means of a digital printing process and is incorporated into the design printed onto the goods.

9. A method according to claim 8, wherein said public data and said private data is incorporated into the design printed onto the goods as reversed out characters, blends or tints.

10. A method marking goods to enable the authenticity of those goods to be verified, wherein a set of public data and a security code are applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm.

11. A method according to claim 10, wherein the public data includes a batch number.

12. A method according to claim 10 or claim 11, wherein the public data includes date information.

13. A method according to any one of claims 10 to 12, wherein said public data and said private data is applied to the goods by means of a digital printing process and is incorporated into the design printed onto the goods.

14. A method according to any one of claims 10 to 13, wherein said public data and said private data is incorporated into the design printed onto the goods as reversed out characters, blends or tints.

15. Goods marked for verification purposes, each of said goods including a set of public data and a security code applied to the goods, said security code having been derived from said public data by means of a predetermined encryption algorithm.

16. Goods according to claim 15, wherein the public data includes a batch number.

17. Goods according to claim 15 or claim 16, wherein the public data includes date information.

18. Goods according to any one of claims 15 to 17, wherein said public data and said private data is applied to the goods by means of a digital printing process and is incorporated into the design printed onto the goods.

19. Goods according to any one of claims 15 to 18, wherein said public data and said private data is incorporated into the design printed onto the goods as reversed out characters, blends or tints.

Fig. 1

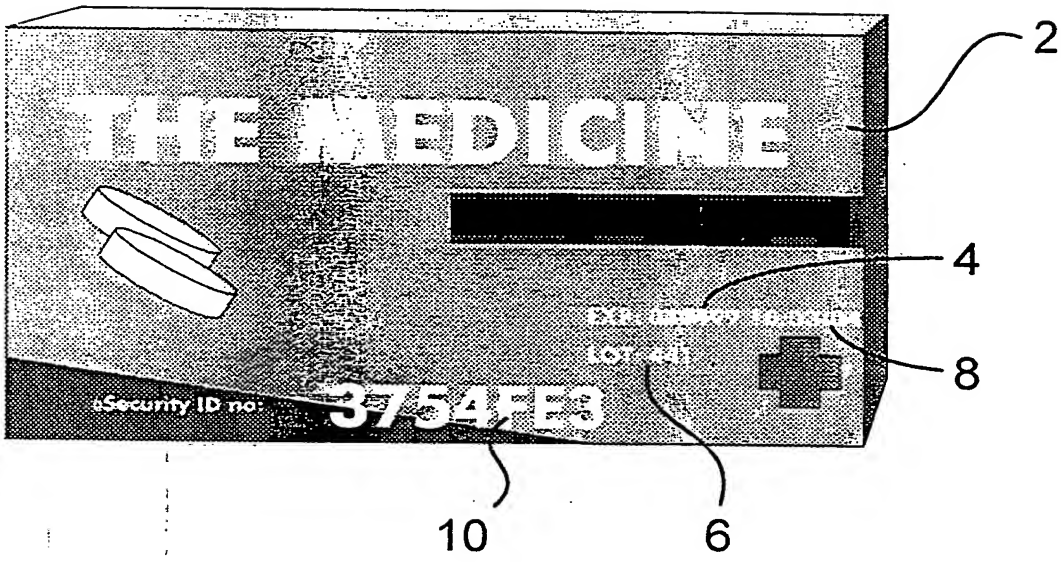


Fig. 2

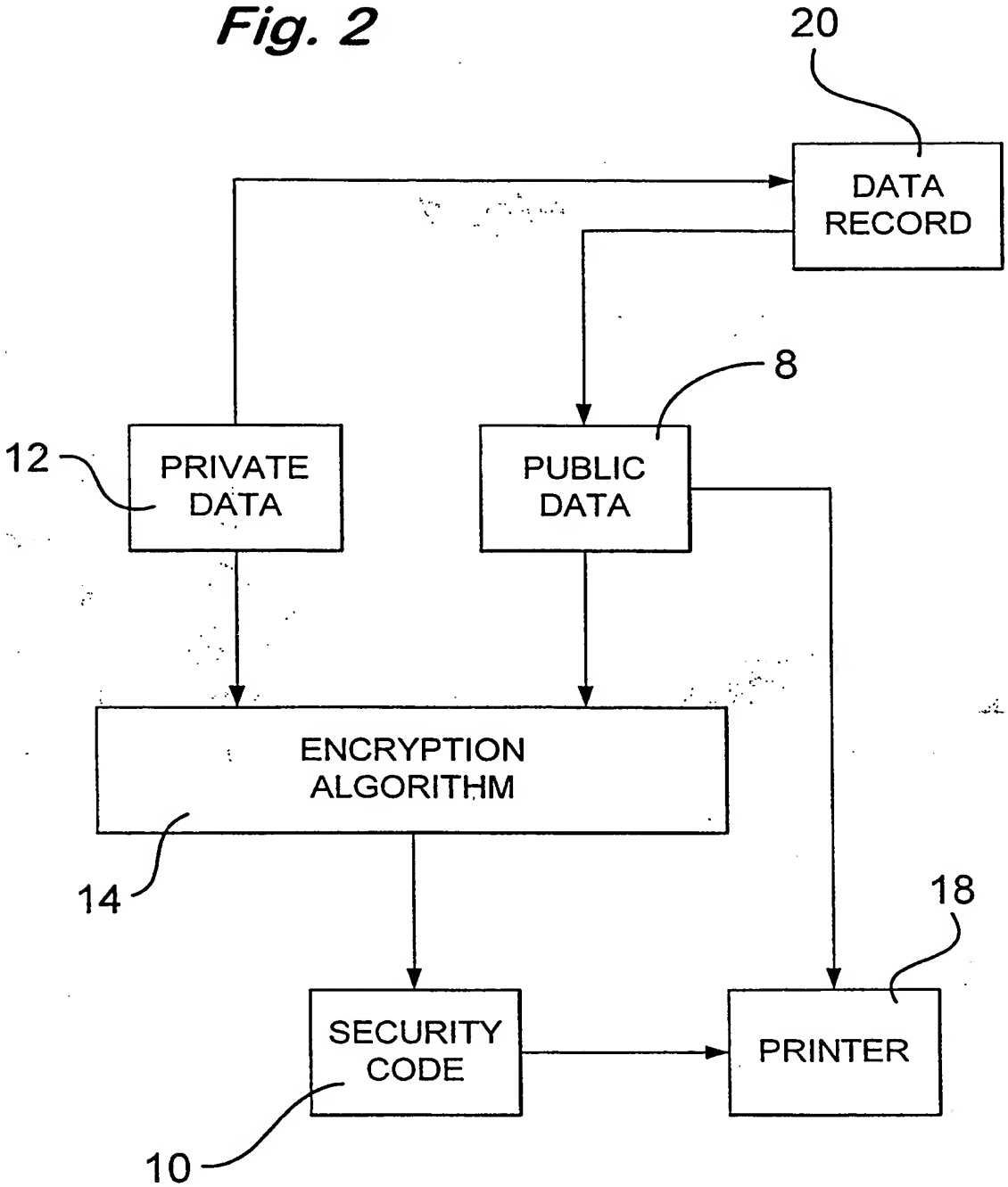
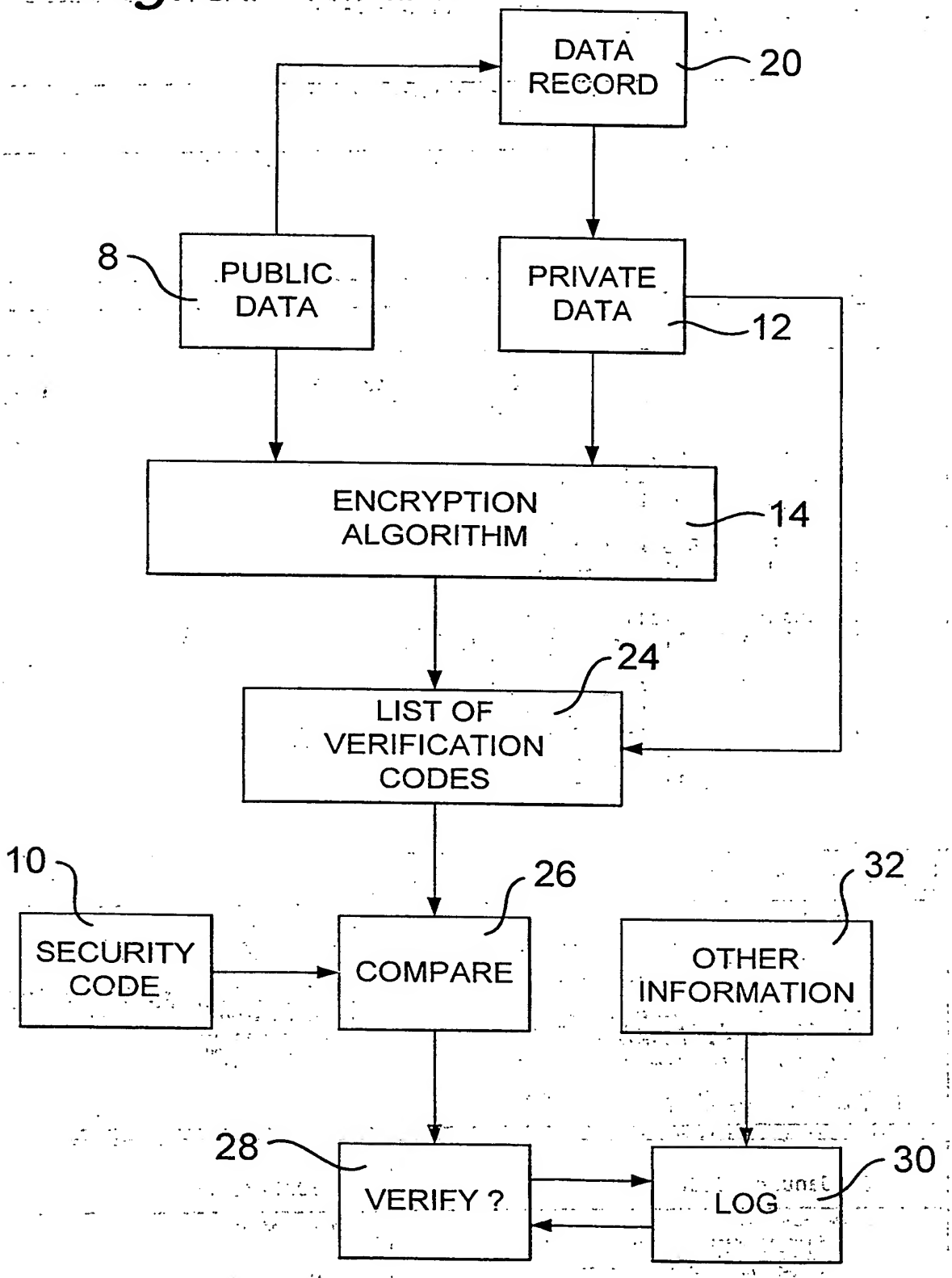


Fig. 3



INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/GB 99/03377

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G07D7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G07D G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 80 02757 A (WINDERLICH H ;STOCKBURGER H (DE)) 11 December 1980 (1980-12-11) abstract; claims; figures page 7, line 10 -page 8, line 3 page 9, line 26 -page 10, line 28	1,5,7, 10,11, 15,16
X	US 5 432 506 A (CHAPMAN THOMAS R) 11 July 1995 (1995-07-11) abstract; claims; figures column 2, line 53 -column 3, line 40	1,2,5-7, 10-12, 15-17
X	US 5 768 384 A (BERSON WILLIAM) 16 June 1998 (1998-06-16) abstract; claims; figures column 2, line 24 - line 63 column 3, line 11 -column 5, line 15	1,10-13, 15-18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 2000	10/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Meyl, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/GB 99/03377

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 388 158 A (BERSON WILLIAM) 7 February 1995 (1995-02-07) abstract; claims; figures column 1, line 43 -column 2, line 63 column 4, line 38 - line 48	10,12,15
A	---	1,2
X,P	EP 0 889 448 A (PITNEY BOWES) 7 January 1999 (1999-01-07) column 3, line 9 -column 4, line 1 column 4, line 40 -column 5, line 42; figures	1,10,12, 15
A	---	
	US 3 833 795 A (INBAR D ET AL) 3 September 1974 (1974-09-03) abstract; claims; figures	1,3,10, 115

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 99/03377

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8002757 A	11-12-1980	DE 2922882 A	11-12-1980
		AT 372211 B	12-09-1983
		AT 904880 A	15-01-1983
		BE 883681 A	01-10-1980
		CA 1161550 A	31-01-1984
		CH 651147 A	30-08-1985
		EP 0030237 A	17-06-1981
		GB 2062340 A,B	20-05-1981
		JP 56500784 T	11-06-1981
		SE 8100649 A	30-01-1981
US 5432506 A	11-07-1995	NONE	
US 5768384 A	16-06-1998	NONE	
US 5388158 A	07-02-1995	CA 2109554 A,C	21-05-1994
		EP 0600646 A	08-06-1994
		JP 7005809 A	10-01-1995
EP 0889448 A	07-01-1999	NONE	
US 3833795 A	03-09-1974	IL 37456 A	15-10-1975
		DE 2237911 A	01-03-1973
		FR 2149863 A	30-03-1973
		JP 48026346 A	06-04-1973
		NL 7210717 A	07-02-1973